



TITLE:

Difference Sets in Generalized Quaternion Groups (Algebraic Combinatorics)

AUTHOR(S):

Hagita, Mariko

CITATION:

Hagita, Mariko. Difference Sets in Generalized Quaternion Groups (Algebraic Combinatorics). 数理解析研究所講究録 1998, 1063: 53-56

ISSUE DATE:

1998-09

URL:

<http://hdl.handle.net/2433/62432>

RIGHT:

Difference Sets in Generalized Quaternion Groups

萩田 真理子 (Mariko Hagita)

Department of Mathematics, Keio University

Abstract

We shall determine all the difference sets in generalized quaternion groups: If there exists a nontrivial difference set D in a generalized quaternion group, then the group is Q_{16} and D is a $(16, 6, 2)$ -difference set.

Existence of difference sets in non-abelian groups are not so much known.

For example, there is a famous conjecture: "There is no nontrivial differences sets in dihedral groups" (see [2],[4]). For known non-abelian difference sets, see [3],[6].

The group

$$Q_{2^l} := \langle a, b \mid a^{2^{l-1}} = 1, bab^{-1} = a^{-1}, b^2 = a^{2^{l-2}} \rangle$$

of order 2^l is called generalized quaternion.

In this paper, we classify all the nontrivial difference sets in Q_{2^l} .

A k -subset D of a group G of order v is called a (v, k, λ) -difference set of G if the list $\{xy^{-1} \mid (x, y) \in D\}$ contains each nonidentity element of G exactly λ times. We call $n := k - \lambda$ the order of D .

We write $\exp(G)$ for the exponent of G .

A prime p is called self-conjugate mod e , if there exists an integer i , such that $p^i \equiv -1 \pmod{e'}$, where e' is the p -free part of e . If each prime divisor of n is self-conjugate mod e , then we say n is self-conjugate mod e .

Let ξ_t be a primitive t -th root of unity and let $[k]$ be the set $\{0, 1, \dots, k-1\}$. The cyclic group Z/kZ and $[k]$ are often identified without explicitly mentioning it.

The following lemma is proved in [1].

Lemma 1 Let $K = Z_u \times Z_w$, where w is an odd integer, $(u, w) = 1, u > 1$. Suppose that $D \in ZK$ satisfies the following conditions for some integer m : (1) $\frac{1}{m}\chi(D)$ is a root of unity for all nontrivial characters χ of K . (2) $\frac{1}{m}\chi_1(D) = \pm 1$ where χ_1 is a character of order uw . (3) $(m, w) = 1$, and (4) m is self-conjugate mod uw . Then

$$\frac{1}{m}\chi(D) = \pm 1$$

holds for any character χ whose order is a multiple of u .

Theorem 2 Suppose D is a $(2^l, k, \lambda)$ -difference set in $G = Q_{2^l}$, then $l = 4, k = 6, \lambda = 2$.

Proof. We may assume that $k < 2^{l-1}$. Then the order $n = k - \lambda$ is a square, since the order of G is even. Let $n = 2^{2i}m^2$, where $2 \nmid m$. Since $\lambda 2^l = k^2 - 2^{2i}m^2$, we see $2^{2i} \mid k^2$. Let $k = 2^i h$. Then $\lambda = k - n = 2^i(h - 2^i m^2) = 2^i \mu$, where $2 \nmid \mu$. Then $2^{l-i-1} \mid h - m$ or $2^{l-i-1} \mid h + m$, since $\mu 2^{l-i} = h^2 - m^2 = (h + m)(h - m)$. Since $m < h < 2^{l-1-i}$, $h + m = 2^{l-i-1}$, $h - m = 2\mu = 2h - 2^{i+1}m^2$. Hence $2^{i+1}m^2 = 2^{l-i-1}$. Then $m = 1, 2^l = 2^{2i+2}$.

Let $D = D_1 + bD_2$, where $D_i = \sum_{k \in 2^{l-1}} d_{ki} a^k$. Then

$$\begin{aligned} DD^{(-1)} &= D_1 D_1^{(-1)} + D_1 D_2^{(-1)} b^{-1} + b D_2 D_1^{(-1)} + b D_2 D_2^{(-1)} b^{-1} \\ &= n + \lambda \langle a \rangle + \lambda b \langle a \rangle. \end{aligned}$$

This implies

$$D_1 D_1^{(-1)} + D_2 D_2^{(-1)} = n + \lambda \langle a \rangle$$

and

$$(1 + a^{2^{l-2}}) D_1 D_2^{(-1)} = \lambda \langle a \rangle = (1 + a^{2^{l-2}}) D_2 D_1^{(-1)}.$$

Let H be a cyclic group of order 2^l generated by g , and

$$E_1 := \sum_{k \in 2^{l-1}} d_{k1} g^{2k}, E_2 := \sum_{k \in 2^{l-1}} d_{k2} g^{2k+1}$$

be elements of ZH . Then

$$E_1 E_1^{(-1)} + E_2 E_2^{(-1)} = n + \lambda \langle g^2 \rangle,$$

$$(1 + g^{2^{l-1}}) E_1 E_2^{(-1)} = \lambda g \langle g^2 \rangle = (1 + g^{2^{l-1}}) E_2 E_1^{(-1)}.$$

Let $p : ZH \rightarrow ZK = ZH/(1, g^{2^{l-1}})$ be the ring homomorphism which is induced by the surjection $H \rightarrow K = H/\{1, g^{2^{l-1}}\}$. Let $\bar{g} = p(g)$, $F_1 = p(E_1)$ and $F_2 = p(E_2)$.

Then

$$F_1 F_1^{(-1)} + F_2 F_2^{(-1)} = n + 2\lambda < \bar{g}^2 >.$$

$$2F_1 F_2^{(-1)} = 2\lambda \bar{g} < \bar{g}^2 > = 2F_2 F_1^{(-1)}.$$

Hence $F = F_1 + F_2 := \sum_{k \in [2^{l-1}]} f_k \bar{g}^k$ satisfies $FF^{(-1)} = n + 2\lambda < \bar{g} >$ and all the coefficients $f_k \in \{0, 1, 2\}$.

Since $n = 2^{2i}$ is self-conjugate mod $\exp(K)$, we see that $\frac{1}{\sqrt{n}}\chi(F)$ is a root of unity for all nontrivial characters χ of K , i.e.,

$$f(\alpha) := \frac{1}{\sqrt{n}} \sum_{k \in [2^{l-1}]} f_k (\eta^\alpha)^k$$

is a root of unity for any $\alpha \in [2^{l-1}] \setminus \{0\}$, where $\eta := \xi_{2^{l-1}}$. We may assume

$$f(1) = \pm 1$$

by translating D if necessary. From Lemma 1, we see

$$f(\alpha) = \pm 1$$

for all $\alpha \in [2^{l-1}]$ such that $(\alpha, 2) = 1$.

Let $A(x)$ be the cyclotomic polynomial of $\xi_{2^{l-1}}$, i.e. $A(x) = x^{2^{l-2}} + 1$. Then the projection

$$h : ZK \longrightarrow ZK/(A(g))$$

satisfies

$$h(F \mp \sqrt{n}) = 0.$$

This means, in ZK ,

$$F \mp \sqrt{n} \text{ is in the principal ideal } (A(g)).$$

Then $|f_k - f_{k+2^{l-2}}| = \sqrt{n}$ for some $k \in [2^{l-2}]$. Hence $\sqrt{n} \leq 2$ follows from $f_k \in \{0, 1, 2\}$.

Since D is a nontrivial difference set, we see $n = 4$ and the only possible parameter is $(v, k, \lambda) = (16, 6, 2)$. \square

Note that $\{1, a, a^2, a^3, b, ba^2\}$ and $\{1, a, a^3, a^4, b, ba^2\}$ are the only non-equivalent (16.6.2)-difference sets in Q_{16} (see [3]). By Theorem 2, these are the only non-trivial difference sets in Q_{2^l} .

However, this result is contained in a nonexistence theorem of difference sets in certain 2-groups (see [5]). We want to generalize this theorem for the group

$$Q_{4l} = \langle a, b \mid a^{2l} = 1, bab^{-1} = a^{-1}, b^2 = a^l \rangle.$$

参考文献

- [1] H.Enomoto, M.Hagita and M.Matsumoto, A note on difference sets, *J.Combin.Theory ser.A*, to appear.
- [2] C.T.Fan, M.K.Siu and S.L.Ma, Difference sets in dihedral groups and interlocking difference sets, *Ars.Combin.* 20A(1985), 99-107.
- [3] R.E.Kibler, A summary of noncyclic difference sets, $k < 20$, *J.Combin.Theory ser.A* 25(1978), 62-67.
- [4] K.H.Leung, S.L.Ma and V.L.Wong, Difference sets in dihedral groups, *Designs. Codes and Cryptography* 1(1991), 333-338.
- [5] R.Liebler, On difference sets in certain 2-groups, *Coding Theory. Design Theory. Group Theory: Proceedings of the Marshall Hall Conference*, ed. by D.Jungnickel. John Wiley and Sons (1993).
- [6] K.W.Smith, Non-abelian Hadamard difference sets, *J.Combin.Theory ser.A* 70(1995), 144-156.